



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,434	05/10/2002	Tomoyuki Asano	SONY JP-181	1147
7590 11/29/2005 Lerner David Littenberg Krumholz & Mentlik 600 South Avenue West Westfield, NJ 07090			EXAMINER DINH, MINH	
			ART UNIT 2132	PAPER NUMBER

DATE MAILED: 11/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/049,434

Applicant(s)

ASANO ET AL.

Examiner

Minh Dinh

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-38 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-38 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10 May 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2/8/02, 3/3/03
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

1. Claims 1-38 have been examined.

Specification

2. The disclosure is objected to because of the following informalities: a typo at the end of line 3 in the abstract, "num er". Appropriate correction is required.

Claim Objections

3. Applicant is advised that should claim 3 be found allowable, claim 4 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 17-20 and 38 are rejected under 35 U.S.C. 101 because the claimed inventions are directed to non-statutory subject matter.

- Regarding claims 17-18, the claimed recording medium is not a computer-readable medium.

- Regarding claim 19, it is not tangibly embodied as it is only software per se; the claimed subject matter, the computer program, is not stored on a computer-readable medium. Claims 20 and 38 are rejected on the same basis.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-11 and 17-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claim 1 recites the limitation "the content" in line 15. There is insufficient antecedent basis for this limitation in the claim. For examination purpose, the limitation is interpreted as "content".
- Claim 7 recites the limitation "the cipher data" in line 10. There is insufficient antecedent basis for this limitation in the claim. For examination purpose, the limitation is interpreted as "cipher data".
- Claim 8 recites the limitations "the plurality information recording devices" in line 2 and "the information recording device" in line 4. There is insufficient antecedent basis for these limitations in the claim. For examination purpose, the limitation is interpreted as "the plurality information reproducing devices" and "the information reproducing device" (see independent claim 7).

Art Unit: 2132

- Similar to claim 8, there is insufficient antecedent basis for the use of "the/said recording device" in claims 9-10. For examination purposes, the device(s) in claims 9-10 are interpreted as the information reproducing device(s) (see independent claim 7).
- Claim 17 recites the limitation "the information" in line 1. There is insufficient antecedent basis for this limitation in the claim. In addition, the claim is generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.
- The claims and the 112, 2nd paragraph problems discussed above are exemplary. There are extensive similar problems in other claims that have not been recited in this Office Action. Applicant is required to go over the whole set of claims to identify and correct these problems.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2132

8. Claims 1-6, 12-13, 17-19, 21, 23-27, 35 and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech (6,609,116) in view of Caronni et al (6,049,878).

Regarding claims 1-2, 12, 17 and 19, Lotspiech discloses an information recording device for recording information on a recording medium, comprising: memory means for holding a device key unique to the information recording device, said memory means also holding a calculate media key command comprising one or more media key blocks which are functionally equivalent to key renewal block(s) formed as renewal key storage data decryptable using the device key; and encryption means for decrypting the key renewal block decryptable using the device key to calculate an encrypting key used in encrypting data to be stored in said recording medium; said encryption means encrypting the data to be stored in said recording medium using the calculated encrypting key; said encryption means detecting, in encrypting and storing the content for said recording medium, the latest usable key renewal block from key renewal blocks stored in said recording medium and from the key renewal block stored in said memory means of the information recording device itself, said encryption means encrypting the data to be stored on said recording medium using the encrypting key obtained on decrypting the detected latest usable key renewal block (col. 4, lines 16-20; col. 5, line 3 – col. 6, line 64). Lotspiech discloses that the information recording device is one of many information recording devices in a system for broadcasting encrypted content (col. 3, lines 18-47); however, Lotspiech does not disclose implementing a key management method using a hierarchical tree structure having nodes each node having a unique

Art Unit: 2132

node key, and a plural number of such information recording devices, operating as leaves, each leaf having a leaf key unique to each information recording device.

Caronni discloses implementing a key management method in a system for broadcasting encrypted content using a hierarchical tree structure having nodes each node having a unique node key, and a plural number of devices, operating as leaves, each leaf having a leaf key unique to each device (col. 4, lines 23-38; col. 6, lines 6-46; col. 8, line 56 – col. 9, line 37). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lotspiech system, device and method to implement a key management method in a system for broadcasting encrypted content using a hierarchical tree structure having nodes each node having a unique node key, and a plural number of devices, operating as leaves, each leaf having a leaf key unique to each device, as taught by Caronni. The motivation for doing so would have been to preserve bandwidth and to minimize computation complexity when updating cryptographic keys (col. 10, lines 36-53). Accordingly, the devices are information recording devices.

Regarding claims 3-4, 13, 21, 24-25, 35 and 38, Lotspiech further discloses detecting the latest key renewal block from key renewal block stored on the recording medium and from the key renewal block stored in the information recording device and writing the latest key renewal block on the recording medium in case the latest key renewal block is the key renewal block stored in the information recording device and the latest key renewal block is not stored on the recording medium (col. 6, lines 22-64).

Regarding claims 5 and 26, Caronni further discloses renewing a node key(s) as claimed, the renewing being implemented using the tree-based key management method discussed in claim 1 (col. 8, line 56 – col. 9, line 37).

Regarding claims 6, 18, 27, Lotspiech further discloses that the encrypting key is associated with a version number as the generation information (col. 5, lines 26-34).

Regarding claims 23 and 37, Lotspiech does not disclose deleting a key renewal block that is not the latest key renewal block. Caronni discloses deleting old key information and storing only the latest key information, the key information being functionally equivalent to a key renewal block (col. 9, lines 51-59). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined device and method of Lotspiech and Hiroshi to delete a key renewal block that is not the latest key renewal block, as taught by Caronni, to achieve forward secrecy and to hinder replay or security attacks.

9. Claims 14, 22 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech in view of Caronni as applied to claims 12, 21 and 35 above, and further in view of Ishiguro (5,796,839). Lotspiech and Hiroshi do not disclose storing the latest key renewal block at the device if the latest key renewal block is stored on the recording medium and has not been stored at the device. Ishiguro discloses storing the latest key information, the latest key information being functionally equivalent to a key renewal block, at the device if the latest key information is stored on the recording medium and has not been stored at the device (col. 7, lines 13-33; col. 8, lines 12-20). It would have

Art Unit: 2132

been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined device and method of Lotspiech and Hiroshi to store the latest key renewal block at the device if the latest key renewal block is stored on the recording medium and has not been stored at the device, as taught by Ishiguro, for ease of encryption key management.

10. Claims 7-11, 15-16 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro in view of Caronni et al (6,049,878).

Regarding claims 7-8, 15 and 20, Ishiguro discloses an information reproducing device for reproducing the information from a recording medium, comprising: memory means for holding renewable key information, the renewable key information being functionally equivalent to key renewal blocks; and encryption means for decrypting the key information using a key provided in said information reproducing device to calculate an encrypting key used for decrypting the cipher data stored in said recording medium; said encryption means decrypting the cipher data stored in said recording medium using the calculated encryption key; said encryption means detecting the one of the key information stored in the recording medium and the key information stored in the memory means of the reproducing device itself, which has a version coincident with the version of the encrypting key of the content to be reproduced; said encryption means executing the decrypting processing of the cipher data stored on the recording medium using the encrypting key obtained by the processing of decrypting the detected key information (col. 3, lines 40-60; col. 4, line 43 – col. 5, line 13; col. 7, lines 20-30; col. 8,

Art Unit: 2132

lines 34-60). Ishiguro not disclose implementing a key management method using a hierarchical tree structure having nodes each node having a unique node key, and a plural number of such information reproducing devices, operating as leaves, each leaf having a leaf key unique to each information recording device. Caronni discloses implementing a key management method using a hierarchical tree structure having nodes each node having a unique node key, and a plural number of devices, operating as leaves, each leaf having a leaf key unique to each device (col. 4, lines 23-38; col. 6, lines 6-46; col. 8, line 56 – col. 9, line 37). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ishiguro device and method to implement a key management method using a hierarchical tree structure having nodes each node having a unique node key, and a plural number of devices, operating as leaves, each leaf having a leaf key unique to each device, as taught by Caronni. The motivation for doing so would have been to preserve bandwidth and to minimize computation complexity when updating cryptographic keys (col. 10, lines 36-53). Accordingly, the devices are information reproducing devices.

Regarding claims 9 and 16, Ishiguro further discloses copying the latest key information from the recording medium to the information reproducing device (col. 7, lines 20-30; col. 8, lines 11-16).

Regarding claim 10, Caronni further discloses renewing a node key(s) as claimed, the renewing being implemented using the tree-based key management method discussed in claim 7 (col. 8, line 56 – col. 9, line 37).

Regarding claim 11, Ishiguro further discloses that the encrypting key is associated with a version number as the generation information (fig. 2).

11. Claims 28-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro in view of Caronni and Lotspiech.

Regarding claims 28-29 and 31-32, Ishiguro discloses an information reproducing device for reproducing the information from a recording medium, comprising: memory means for holding renewable key information, the renewable key information being functionally equivalent to key renewal blocks; and encryption means for decrypting the key information using a key provided in said information reproducing device to calculate an encrypting key used for decrypting the cipher data stored in said recording medium; said encryption means decrypting the cipher data stored in said recording medium using the calculated encryption key; said encryption means detecting the one of the key information stored in the recording medium and the key information stored in the memory means of the reproducing device itself, which has a version coincident with the version of the encrypting key of the content to be reproduced; said encryption means executing the decrypting processing of the cipher data stored on the recording medium using the encrypting key obtained by the processing of decrypting the detected key information (col. 3, lines 40-60; col. 4, line 43 – col. 5, line 13; col. 7, lines 20-30; col. 8, lines 34-60).

Ishiguro does not disclose implementing a key management method using a hierarchical tree structure having nodes each node having a unique node key, and a

Art Unit: 2132

plural number of such information reproducing devices, operating as leaves, each leaf having a leaf key unique to each information recording device. Caronni discloses implementing a key management method using a hierarchical tree structure having nodes each node having a unique node key, and a plural number of devices, operating as leaves, each leaf having a leaf key unique to each device (col. 4, lines 23-38; col. 6, lines 6-46; col. 8, line 56 – col. 9, line 37). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ishiguro device and method to implement a key management method using a hierarchical tree structure having nodes each node having a unique node key, and a plural number of devices, operating as leaves, each leaf having a leaf key unique to each device, as taught by Caronni. The motivation for doing so would have been to preserve bandwidth and to minimize computation complexity when updating cryptographic keys (col. 10, lines 36-53). Accordingly, the devices are information reproducing devices.

Ishiguro does not disclose renewal means for comparing, in accessing the recording medium, the version of a key renewal block stored in the recording medium to that of the key renewal block owned by the reproducing device itself, and for writing the key renewal block of the new version in the recording medium, if the key renewal block of the new version is the key renewal block stored in the memory means of reproducing device itself, and the key renewal block of the new version is not as yet stored on the recording medium. Lotspiech discloses a recording/reproducing device comprises renewal means for comparing, in accessing a recording medium, the version of a key renewal block stored in the recording medium to that of the key renewal block owned by

Art Unit: 2132

the reproducing device itself, and for writing the key renewal block of the new version in the recording medium, if the key renewal block of the new version is the key renewal block stored in the memory means of recording/reproducing device itself, and the key renewal block of the new version is not as yet stored on the recording medium (col. 6, line 22 – col. 7, line 6). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ishiguro device to comprise renewal means for comparing, in accessing the recording medium, the version of a key renewal block stored in the recording medium to that of the key renewal block owned by the reproducing device itself, and for writing the key renewal block of the new version in the recording medium, if the key renewal block of the new version is the key renewal block stored in the memory means of reproducing device itself, and the key renewal block of the new version is not as yet stored on the recording medium, as taught by Lotspiech. The motivation for doing so would have been that new key information could be transmitted to valid devices that share a revoked key with compromised devices.

Regarding claim 30, Ishiguro does not disclose deleting a key renewal block that is not the latest key renewal block. Caronni discloses deleting old key information and storing only the latest key information, the key information being functionally equivalent to a key renewal block (col. 9, lines 51-59). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Ishiguro device to delete a key renewal block that is not the latest key renewal block, as taught by Caronni, to achieve forward secrecy and to hinder replay or security attacks.

Regarding claim 33, Caronni further discloses renewing a node key(s) as claimed, the renewing being implemented using the tree-based key management method discussed in claim 28 (col. 8, line 56 – col. 9, line 37).

Regarding claim 34, Ishiguro further discloses that the encrypting key is associated with a version number as the generation information (fig. 2).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,832,319 to Bell et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

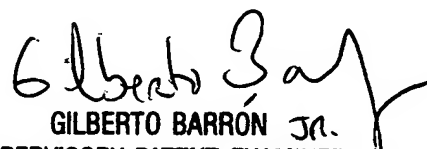
Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
11/25/05


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100